FIPS 201 Evaluation Program - Authentication Key Reader Test Procedure

Version 2.0.0
June 30, 2006

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	03/20/06	Document creation.	Limited
Draft	0.1.0	03/21/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	04/21/06	Updated based on feedback from GSA.	Limited
Draft	0.2.0	04/21/06	Submitted to GSA for approval.	GSA
Draft	0.2.1	05/19/06	Updated based on feedback from GSA.	Limited
Draft	0.2.2	05/22/06	Updated based on feedback from GSA.	Limited
Approved	1.0.0	05/23/06	Approved by GSA.	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA.	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval.	GSA
Approved	2.0.0	06/30/06	Approved by GSA.	Public

Table of Contents

List of Tables

List of Figures

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Authentication Key Reader (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product being compliant to the applicable requirements of FIPS 201. The Product must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the Product in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product as conformant to the requirements of FIPS 201.

3 Test Procedure for Authentication Key Reader

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product. The different test cases that are used to check compliance to the requirements is also cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
R-AUK.3	PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	Card /Card Reader Interoperability Requirements, Section 2.2.2.2	R-AUK-TP.1
R-AUK.4	The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.	Card /Card Reader Interoperability Requirements, Section 2.2.2.3	R-AUK-TP.2
R-AUK.9	The PIV Authentication Certificate received from the reader shall be the data that was written by the lab on each “Golden” test card.	Derived Test Requirement	R-AUK-TP.3
R-AUK.10	The reader shall be able to generate and send a cryptographic challenge to the PIV Card.	FIPS 201 Section 6.2.4	R-AUK-TP.4
R-AUK.11	The reader shall be able to decrypt and match the cryptographic response from the PIV Card.	FIPS 201 Section 6.2.4	R-AUK-TP.4

Table 1 - Applicable Requirements

3.2 Test Components

3.2.1 Baseline Configuration

The baseline configuration describes initial state of the Card Reader Test Fixture and its associated components. A Lab Engineer commences execution of this test procedure after performing the necessary updates to the baseline configuration based on the requirements of the test cases described below.

The Card Reader Test Fixture includes the following components as part of its baseline configuration:

1. The Host System – It includes the workstation and the Test Application software.
2. Breakout Box – The USB and Serial Communication cables from the breakout box are connected to the Host System.

Figure 1 provides an illustration of the baseline configuration for the Card Reader Test Fixture.

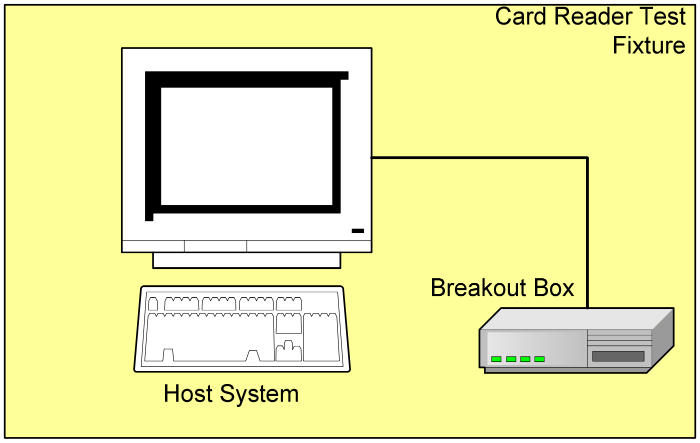


Figure 1 - Card Reader Test Fixture Baseline Configuration

3.2.2 Components Details

Table 2 provides the details of all the components required by the Lab to execute this test procedure. Based on the different test cases, different components may be required to execute the test case.

#	Component	Component Details	Identifier
1	The Card Reader Test Fixture	-	CRTF
2	Authentication Key Reader under test	-	PROD
3	A PIV Card that supports the Class A operating Class only	Gemplus GemCombi Xpresso R4 E72K PK card with the Gemplus GemPIV applet v1.01	PCARD-CLA
4	A PIV Card that supports the T=0 transmission protocol only	Gemplus GemCombi Xpresso R4 E72K PK card with the Gemplus GemPIV applet v1.01	PCARD-T0

#	Component	Component Details	Identifier
5	A PIV Card that supports the T=1 transmission protocol only	SafeNet Model 400 Smart Card (72K) SCCOS Version 3.0 with PIV card application	PCARD-T1

Table 2 - Test Procedure: Components

3.3 Test Cases

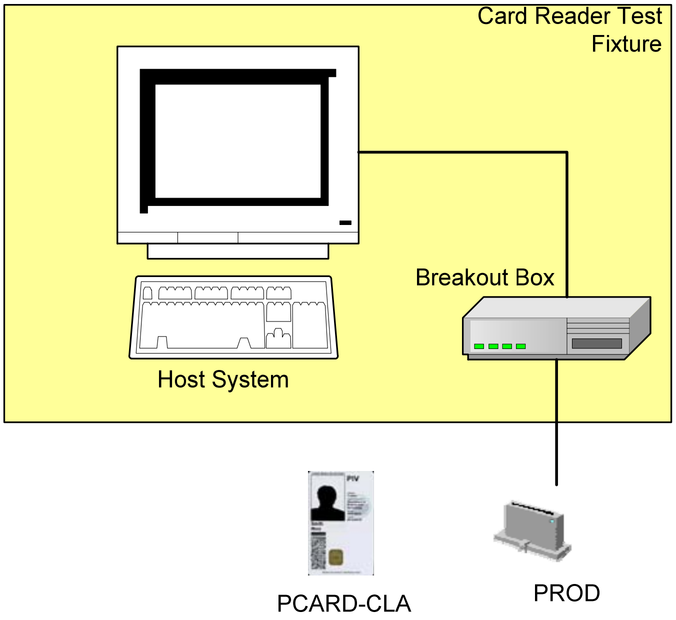
This section discusses the various test cases that are needed to test the Product against the requirements mentioned above.

3.3.1 Test Case R-AUK-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that the PIV reader supports the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

3.3.1.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-CLA ▪ PROD
Configuration Diagram :	 Card Reader Test Fixture Breakout Box Host System PCARD-CLA PROD **Figure 2 - Configuration Diagram for Test Case R-AUK-TP.1**

Preparation	▪ Install the drivers for the PROD in accordance with the manufacturer provided documentation. ▪ Connect the PROD into the appropriate port in the breakout box of the CRTF. ▪ Verify that the PROD is correctly installed by reviewing its presence in list of hardware using the device manager of the host system.

3.3.1.3 Test Process

Test Steps:	1. Execute the Test Application on the CRTF. 2. Make sure that the details of PCARD-CLA are entered into the Test Application using the File → Edit Reference Contact Card Implementation Info 3. Select the tab for the "Authentication Key Reader". This selects the test for the Authentication Key Reader in the Test Application. (See Figure 6 - Testing Screen for the Authentication Key Reader) 4. Fill in all the information as required in the screen for the testing PROD as shown in Figure 3. 5. Select the Test Case radio button corresponding to R-AUK-TP.1 6. Insert PCARD-CLA into PROD. 7. Click on the "Execute Test" button. Follow the steps on the screen. 8. Verify that the test was completed by reviewing the result on the screen. (See Figure 8 - Test Report for the Authentication Key Reader)
Expected Result(s):	1. The test completes successfully showing that the Authentication Key Reader supports Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.

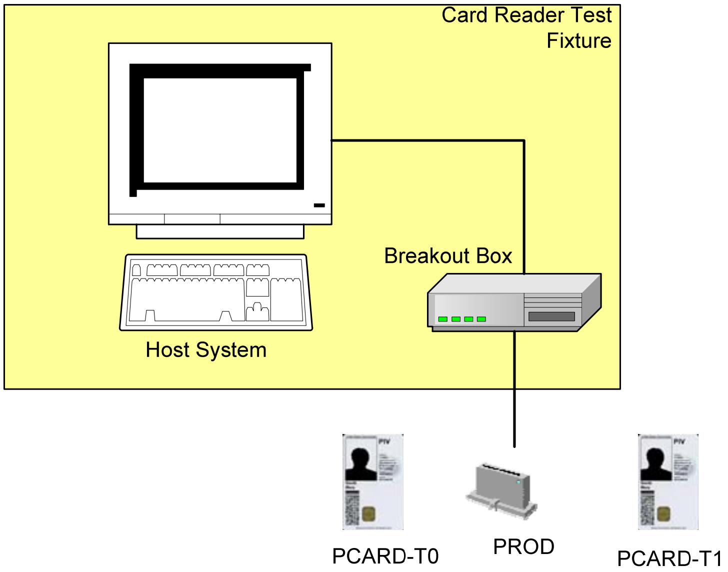
3.3.2 Test Case R-AUK-TP.2

3.3.2.1 Purpose

The purpose of this test is to verify that the contact interface of the reader supports both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.

3.3.2.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-T0 ▪ PCARD-T1 ▪ PROD

Configuration Diagram:	 Card Reader Test Fixture Breakout Box Host System PCARD-T0 PROD PCARD-T1 **Figure 3 - Configuration Diagram for Test Case R-AUK-TP.2**
Preparation:	▪ No further preparation required in addition to that described in Test Case R-AUK-TP.1

3.3.2.3 Test Process

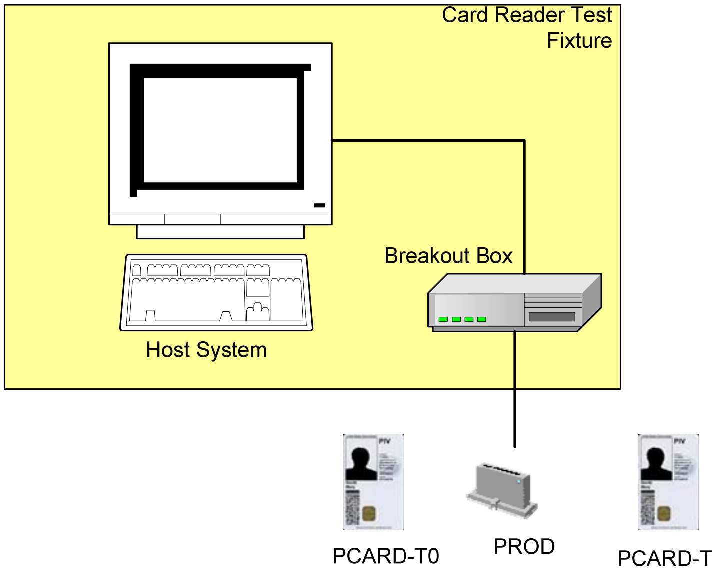
Test Steps:	1. Select the Test Case radio button corresponding to R-AUK-TP.2 2. Make sure that the details of PCARD-T0 and PCARD-T1 are entered into the Test Application using the File → Edit Reference Contact Card Implementation Info 3. Insert PCARD-T0 into PROD. 4. Click on the "Execute Test" button. Follow the steps on the screen. 5. When prompted, insert PCARD-T1 into PROD. 6. Click the "OK" button to proceed. 7. Verify that the test was completed by reviewing the result on the screen. (See Figure 8 - Test Report for the Authentication Key Reader)
Expected Result(s):	1. The test completes successfully showing that the Authentication Key Reader supports both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997.

3.3.3 Test Case R-AUK-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the data received from the PIV Authentication Key reader is the data that was loaded onto the "Golden" cards, and not corrupted during transmission.

3.3.3.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-T0 ▪ PCARD-T1 ▪ PROD
Configuration Diagram:	 Card Reader Test Fixture Breakout Box Host System PCARD-T0 PROD PCARD-T1 **Figure 4 - Configuration Diagram for Test Case R-AUK-TP.3**
Preparation:	▪ Generate test data that resembles a PIV Authentication Certificate. ▪ Load the data into the <*configuration file*> for PCARD-T0 and PCARD-T1.

3.3.3.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-AUK-TP.3 2. Make sure that the details of PCARD-T0 and PCARD-T1 are entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window (See Figure 7 - Reference Card Information). 3. Insert PCARD-T0 into PROD.

	4. Click on the "Execute Test" button. Follow the steps on the screen. 5. When prompted, insert PCARD-T1 into PROD. 6. Click the "OK" button to proceed. 7. Verify that the test was completed by reviewing the result on the screen. (See Figure 8 - Test Report for the Authentication Key Reader)
Expected Result(s):	1. The test completes successfully showing that the PIV Authentication Key reader has passed the data that was placed on PCARD-T0 and PCARD-T1 to CRTF.

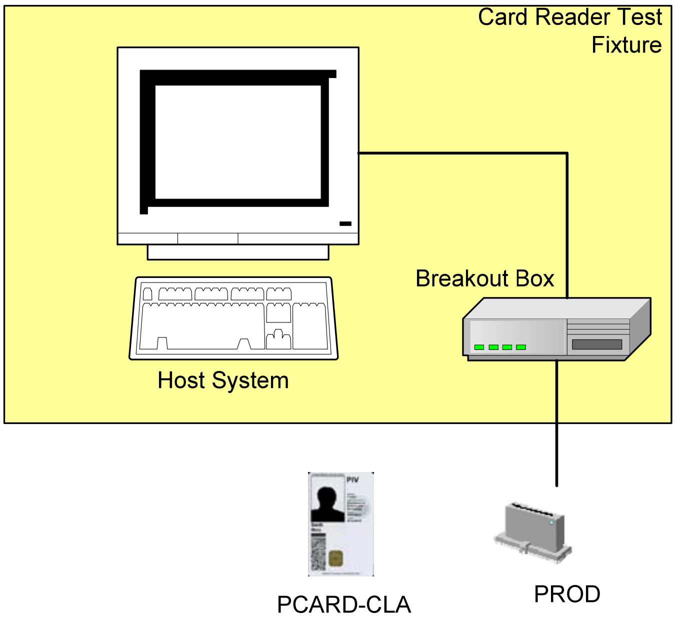
3.3.4 Test Case R-AUK-TP.4

3.3.4.1 Purpose

The purpose of this test is to verify that the PIV Authentication Key Reader has generated and sent a cryptographic challenge to the PIV Card. The test will also verify that the PIV Authentication Key Reader has verified that the Private Key has been used to encrypt the challenge. This is performed using a mismatched public/private keypair and verifying that authentication is not possible.

3.3.4.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-CLA ▪ PROD

Configuration Diagram:	 Card Reader Test Fixture Breakout Box Host System PCARD-CLA PROD **Figure 5 - Configuration Diagram for Test Case R-AUK-TP.4**
Preparation:	▪ With the PIV Card inserted into a smart card reader, fire the SP 800-73 Card Command APDU, Generate Asymmetric Key Pair (0047009A) ▪ Generate a PIV Authentication Certificate using a Public Key value other than what was given as a response to the previous step. ▪ Load the PIV Authentication Certificate onto the PIV Card in the appropriate buffer. (i.e. containerID 5FC105)

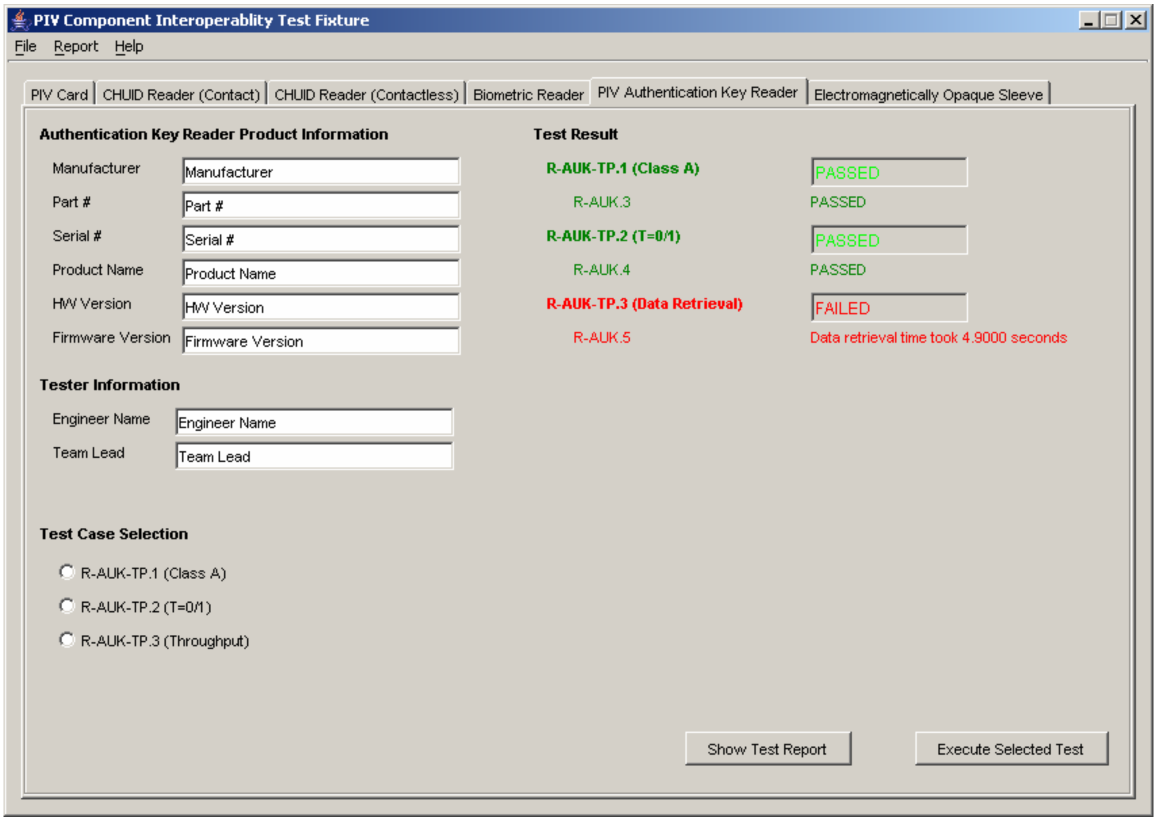
3.3.4.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-AUK-TP.4 2. Make sure that the details of PCARD-CLA is entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window (See Figure 7 - Reference Card Information). 3. Insert PCARD-CLA into PROD. 4. Verify that the test was completed by reviewing the result on the screen. (See Figure 8 - Test Report for the Authentication Key Reader)
Expected Result(s):	1. The test completes successfully showing that the PIV Authentication Key reader has generated a cryptographic challenge and sent it to the card, the response has been decrypted and authentication has failed.

4 Authentication Key Reader Test Application Screens

4.1 Testing Screen

The following represents a screen shot of the Test Application that is used when testing an Authentication Key Reader. The Lab Engineer is expected to manually provide the information for **Authentication Key Reader Product Information**, **Tester Information,** and **Test Case Selection** when completing testing.


PIV Component Interoperablity Test Fixture
File
Report
Help
PIV Card
CHUID Reader (Contact)
CHUID Reader (Contactless)
Biometric Reader
PIV Authentication Key Reader
Electromagnetically Opaque Sleeve
Show Test Report
Execute Selected Test

Authentication Key Reader Product Information

Manufacturer	Manufacturer
Part #	Part #
Serial #	Serial #
Product Name	Product Name
HW Version	HW Version
Firmware Version	Firmware Version

Tester Information

Engineer Name	Engineer Name
Team Lead	Team Lead

Test Case Selection

○ R-AUK-TP.1 (Class A)
○ R-AUK-TP.2 (T=0/1)
○ R-AUK-TP.3 (Throughput)

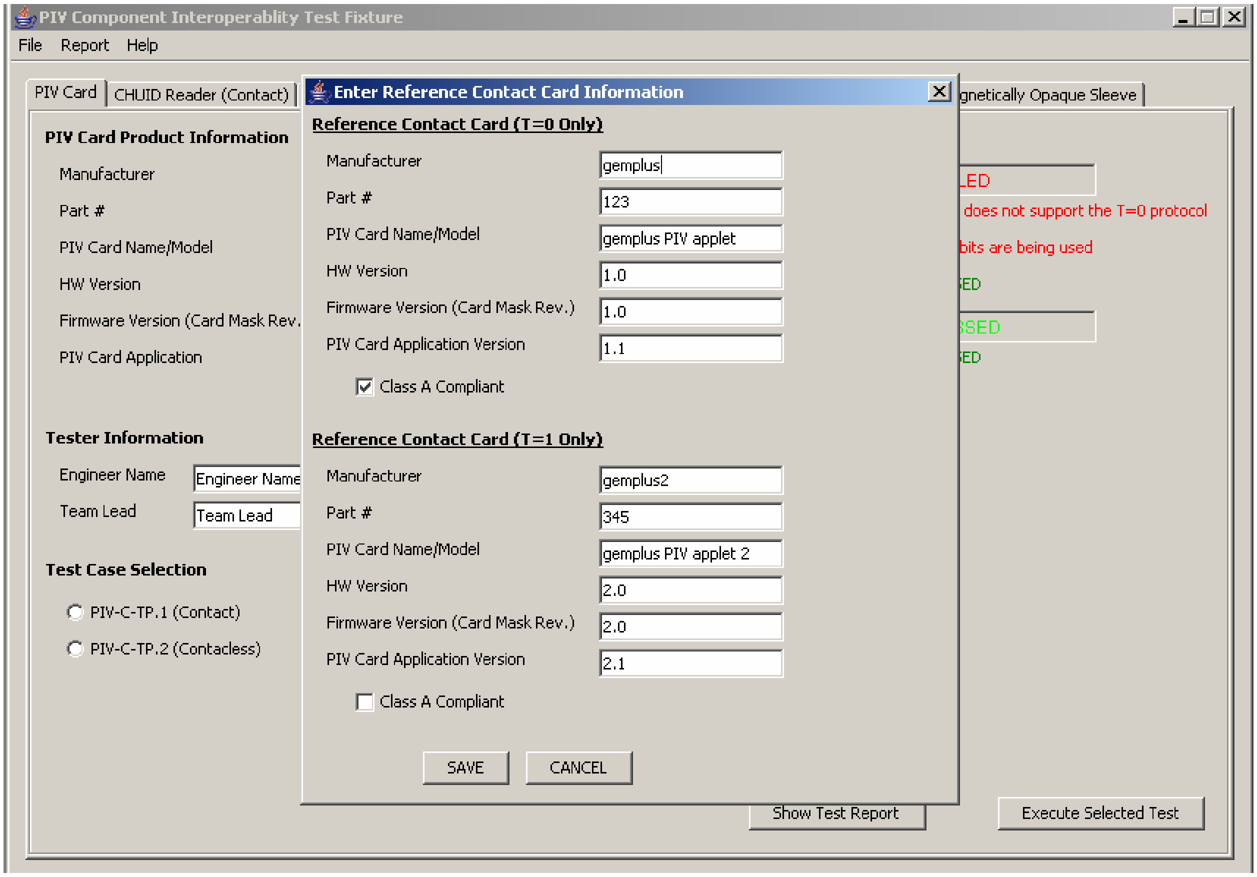
Test Result

R-AUK-TP.1 (Class A)	PASSED
R-AUK.3	PASSED
R-AUK-TP.2 (T=0/1)	PASSED
R-AUK.4	PASSED
R-AUK-TP.3 (Data Retrieval)	FAILED
R-AUK.5	Data retrieval time took 4.9000 seconds

Figure 6 - Testing Screen for the Authentication Key Reader

4.2 Reference Card Information

The following screen shot depicts the configuration window that will need to be edited to contain the details of the PIV Cards used during testing. Lab Engineers are expected to fill in all fields listed in this window prior to beginning the applicable test.



Tester Information

Engineer Name: Engineer Name

Team Lead: Team Lead

Test Case Selection

○ PIV-C-TP.1 (Contact)

○ PIV-C-TP.2 (Contacless)

Enter Reference Contact Card Information

Reference Contact Card (T=0 Only)

Manufacturer	gemplus
Part #	123
PIV Card Name/Model	gemplus PIV applet
HW Version	1.0
Firmware Version (Card Mask Rev.)	1.0
PIV Card Application Version	1.1

☑ Class A Compliant

Reference Contact Card (T=1 Only)

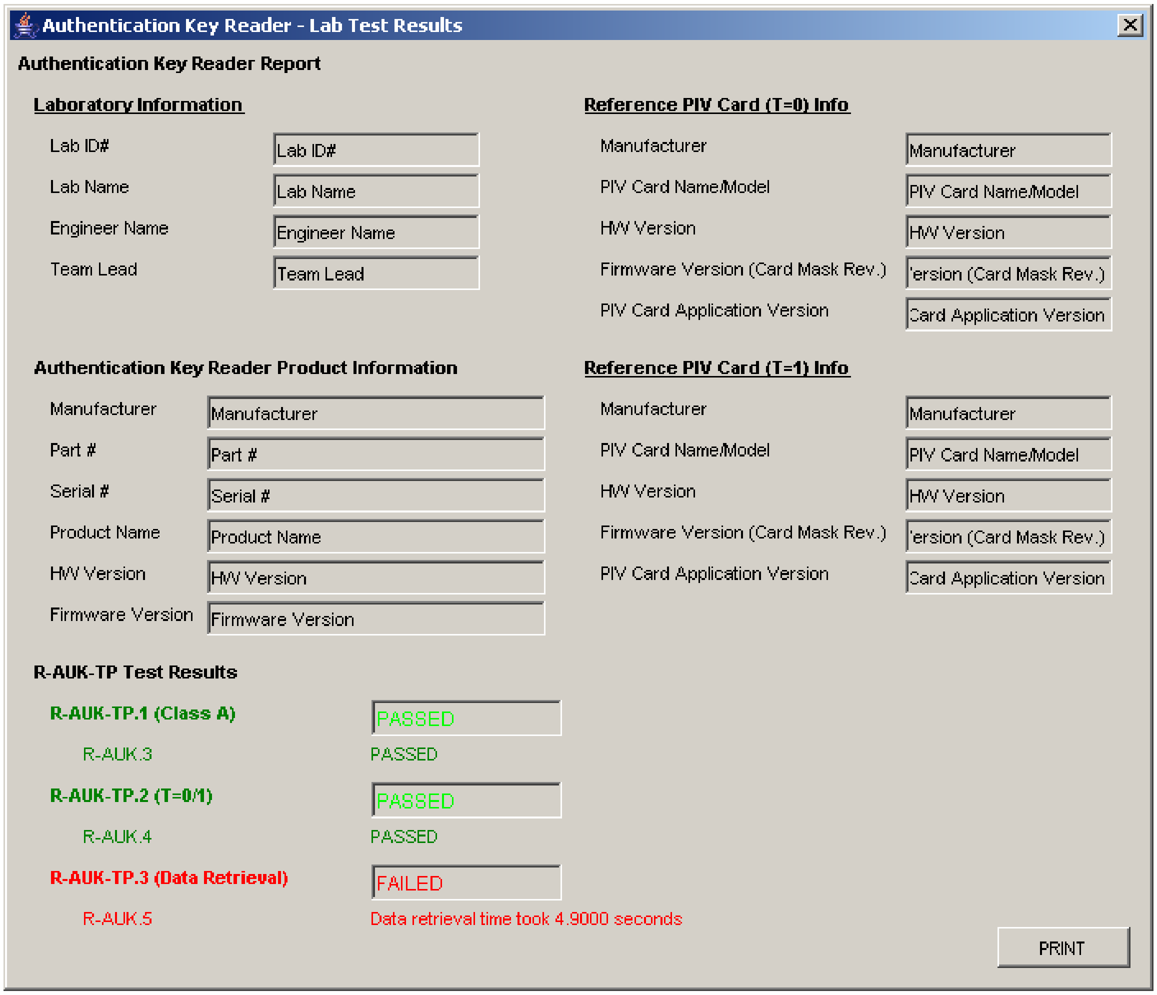
Manufacturer	gemplus2
Part #	345
PIV Card Name/Model	gemplus PIV applet 2
HW Version	2.0
Firmware Version (Card Mask Rev.)	2.0
PIV Card Application Version	2.1

☐ Class A Compliant

Figure 7 - Reference Card Information

4.3 Test Report Screen

The following represents a screen shot of the test report that is generated by the Test Application after the Authentication Key Reader testing has been completed. It provides the Lab Engineer with a reference of what to expect as a result of successful execution of the test procedure. A Lab Engineer is not expected to fill out any portion of the report manually.



Authentication Key Reader - Lab Test Results

Authentication Key Reader Report

Laboratory Information

Lab ID#	Lab ID#
Lab Name	Lab Name
Engineer Name	Engineer Name
Team Lead	Team Lead

Reference PIV Card (T=0) Info

Manufacturer	Manufacturer
PIV Card Name/Model	PIV Card Name/Model
HW Version	HW Version
Firmware Version (Card Mask Rev.)	'ersion (Card Mask Rev.)
PIV Card Application Version	Card Application Version

Authentication Key Reader Product Information

Manufacturer	Manufacturer
Part #	Part #
Serial #	Serial #
Product Name	Product Name
HW Version	HW Version
Firmware Version	Firmware Version

Reference PIV Card (T=1) Info

Manufacturer	Manufacturer
PIV Card Name/Model	PIV Card Name/Model
HW Version	HW Version
Firmware Version (Card Mask Rev.)	'ersion (Card Mask Rev.)
PIV Card Application Version	Card Application Version

R-AUK-TP Test Results

R-AUK-TP.1 (Class A)	PASSED
R-AUK.3	PASSED
R-AUK-TP.2 (T=0/1)	PASSED
R-AUK.4	PASSED
R-AUK-TP.3 (Data Retrieval)	FAILED
R-AUK.5	Data retrieval time took 4.9000 seconds

Figure 8 - Test Report for the Authentication Key Reader